What is claimed is:

1. A device, used in a communication apparatus, for securing an information associated with a subscriber, said communication apparatus comprising a cipher-key generating module for generating a cipher key, said device comprising:

   a storage module, which the information associated with the subscriber, is stored in;

   a cipher-key acquiring module for transmitting an input to the cipher-key generating module, and then receiving the cipher key generated by the cipher-key generating module in response to the input;

   an encrypting module for retrieving the cipher key through the cipher-key acquiring module, retrieving the information associated the subscriber from the storage module, and encrypting the information associated with the subscriber using the cipher key to generate an encrypted information, wherein after generated, the encrypted information is stored in the storage module and replaces the information associated with the subscriber stored in the storage module; and

   a decrypting module for retrieving the cipher key through the cipher-key acquiring module, retrieving the encrypted information from the storage module, and decrypting the encrypted information using the cipher key to recover the information associated with the subscriber when the information associated with the subscriber needs to be used, and wherein when the decrypting module retrieves the cipher key through the cipher-key acquiring module, the cipher-key acquiring module transmits the input once more to the cipher-key generating module, and then receives the cipher key generated once more by the cipher-key generating module in response to the input.

2. The device of claim 1, wherein the input is a hardware serial number resident in the communication apparatus.

3. The device of claim 1, wherein the cipher-key generating module previously stores a subscriber code, and the cipher-key generating module outputs the subscriber code as the cipher key in response to the input.

4. The device of claim 1, where the cipher-key generating module is a SIM (Subscriber Information Module) card.

5. The device of claim 1, wherein the encrypting module and the decrypting module are implemented in the same module.

6. The device of claim 1, wherein the cipher-key generating module has a predetermined algorithm, and the input is applied into the predetermined algorithm to generate the cipher key.

7. The device of claim 6, wherein the predetermined algorithm is one selected from the group consisting of an HMAC (Hash-based Message Authentication Code) algorithm, a GSM-A3 algorithm and a GSM-A8 algorithm.

8. A device, used in a communication apparatus, for securing an information associated with a subscriber, said communication apparatus comprising a cipher-key generating module for generating a cipher key, said device comprising:

a storage module which the information associated with the subscriber is stored in;

a random input generating module for generating a random input;

a cipher-key acquiring module for receiving the random input from the random data generating module, transmitting the random input to the cipher-key generating module, and then receiving the cipher key generated by the cipher-key generating module in response to the random input;

an encrypting module for retrieving the cipher key through the cipher-key acquiring module, retrieving the information associated the subscriber from the storage module, and encrypting the information associated with the subscriber using the cipher key to generate an encrypted information, wherein after generated, the encrypted information is stored together with the random input in the storage module and replaces the information associated with the subscriber stored in the storage module; and

a decrypting module for retrieving the cipher key through the cipher-key acquiring module, retrieving the encrypted information from the storage module, and decrypting the encrypted information using the cipher key to recover the information associated with the subscriber when the information associated with the subscriber needs to be used, and wherein when the decrypting module retrieves the cipher key through the cipher-key acquiring module, the cipher-key acquiring module retrieves the random input stored in the storage module, transmits the random input once more to the cipher-key generating module, and then receives the cipher key generated once more by the cipher-key generating module in response to the random input.

9. The device of claim 8, wherein the cipher-key generating module has a predetermined algorithm, and the random input is applied into the predetermined algorithm to generate the cipher key.

10. The device of claim 9, where the cipher-key generating module is a SIM (Subscriber Information Module) card.

11. The device of claim 10, wherein the predetermined algorithm is one selected from the group consisting of an HMAC (Hash-based Message Authentication Code) algorithm, a GSM-A3 algorithm and a GSM-A8 algorithm.

12. The device of claim 11, wherein the encrypting module and the decrypting module are implemented in the same module.

13. A method, performed in a communication apparatus, for securing an information associated with a subscriber, said communication apparatus comprising a cipher-key generating module for generating a cipher key, said method comprising the steps of:

transmitting an input to the cipher-key generating module;

receiving the cipher key generated by the cipher-key generating module in response to the input;

encrypting the information associated with the subscriber using the cipher key to generate an encrypted information; and

when the information associated with the subscriber needs to be used, transmitting the input once more to the cipher-key generating module, receiving the cipher key generated once more by the cipher-key generating module in response to the input, and decrypting the encrypted information using the cipher key to recover the information associated with the subscriber.

14. The method of claim 13, wherein the input is a hardware serial number resident in the communication apparatus.

15. The method of claim 13, wherein the cipher-key generating module has a predetermined algorithm, and the input is applied into the predetermined

algorithm to generate the cipher key.

16. The method of claim 13, wherein the cipher-key generating module previously stores a subscriber code, and outputs the subscriber code as the cipher key in response to the input.

17. The method of claim 13, where the cipher-key generating module is a SIM (Subscriber Information Module) card.

18. The method of claim 17, wherein the predetermined algorithm is one selected from the group consisting of an HMAC (Hash-based Message Authentication Code) algorithm, a GSM-A3 algorithm and a GSM-A8 algorithm.

19. A method, performed in a communication apparatus, for securing an information associated with a subscriber, said communication apparatus comprising a cipher-key generating module for generating a cipher key, said method comprising the steps of:

generating a random input;

transmitting the random input to the cipher-key generating module;

receiving a cipher key generated by the cipher-key generating module in response to the random input;

encrypting the information associated with the subscriber using the cipher key to generate an encrypted information; and

when the information associated with the subscriber needs to be used, transmitting the random input once more to the cipher-key generating module, receiving the cipher key generated once more by the cipher-key generating module in response to the random input, and decrypting the encrypted information using the cipher key to recover the information associated with the subscriber.

20. The method of claim 19, wherein the cipher-key generating module has a predetermined algorithm, and the random input is applied into the predetermined algorithm to generate the cipher key.

21. The method of claim 20, where the cipher-key generating module is a SIM (Subscriber Information Module) card.

22. The method of claim 21, wherein the predetermined algorithm is one selected from the group consisting of an HMAC (Hash-based Message Authentication Code) algorithm, a GSM-A3 algorithm and a GSM-A8 algorithm.